UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ALEXANDRA O'BRIEN, JASON O'BRIEN, MARY GORMAN, ELIZABETH AMES and MARY HOPE GRIFFIN, individually and on behalf of all others similarly situated, Plaintiffs, v. HOME DEPOT U.S.A., INC., a Delaware corporation; and DOES 1-50, Defendants.	**CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED Case No. 14-cv- 5301

Plaintiffs Alexandra O'Brien, Jason O'Brien, Mary Gorman, Elizabeth Ames and Mary Hope Griffin ("Plaintiffs") bring this class action against Defendant Home Depot U.S.A., Inc. ("Home Depot" or "Defendant") and DOES 1-50 (collectively, "Defendants") on behalf of themselves and all others similarly situated to obtain damages, restitution, and injunctive relief for the Class, as defined, below, from Defendants. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant Home Depot U.S.A., Inc. for failing to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), personally identifiable information such as names, mailing addresses, email addresses and other personal information ("PII") (collectively, "Private Information"), and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen and precisely what types of information were stolen (the "Data

Breach").

2. On September 8, 2014, Home Depot confirmed that it allowed a massive breach of its customers' Private Information to occur in 2014.

3. Home Depot disregarded Plaintiffs' and Class Members' rights by intentionally, willfully, recklessly, or negligently failing to take the necessary precautions required to safeguard and protect their Private Information from unauthorized disclosure. On information and belief, Plaintiffs' and Class Members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class Members' Private Information was compromised and stolen.

4. Plaintiffs bring this lawsuit on behalf of themselves and all others similarly situated alleging that Defendant violated the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x ("FCRA"); New York General Business Law § 349, the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, failed to expediently notify Plaintiffs and Class Members following the security breach in violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-2 *et seq.*, violated the Illinois Personal Information Protection Act, 815 ILCS 530, *et seq.*, breached its contract with Plaintiffs and Class Members; acted negligently; and was unjustly enriched.

PARTIES

5. Plaintiff Alexandra O'Brien is an individual who resides in Suffolk County, New York. Plaintiff A. O'Brien used a credit card to purchase goods on September 3, 2014 and between April 2014 and September 2014 at Home Depot stores in Nassau and Suffolk counties in New York State.

6. Plaintiff Jason O'Brien is an individual who resides in Suffolk County, New York. Plaintiff J. O'Brien used a credit card to purchase goods between April 2014 and September 2014 at Home Depot stores in Nassau and Suffolk counties in New York State.

7. Plaintiff Mary Gorman is an individual who resides in Essex County, New Jersey. Plaintiff Gorman used a debit card between April 2014 and September 2014 to purchase goods at Home Depot stores in New Jersey, primarily the Union/Vauxhall Store #915 located in 2445 Springfield Avenue, Vauxhall, NJ 07088. Plaintiff Gorman had occasion to return some but not all merchandise during this time.

8. Plaintiff Mary Hope Griffin is an individual who resides in Cook County in Illinois. Plaintiff Griffin used a credit card for purchases in Home Depot stores between April 2014 and September 2014 to purchase goods at stores in Illinois.

9. Plaintiff Elizabeth Ames is an individual who resides in Essex County, New Jersey. Plaintiff Ames used a Home Depot credit card, as well as other credit cards, between April 2014 and September 2014 to purchase goods at Home Depot stores in New Jersey. Plaintiff Ames had occasion to return some, but not all, purchased merchandise during this time.

10. Defendant Home Depot U.S.A., Inc. is a Delaware corporation headquartered in Atlanta, Georgia. Defendant operates retail stores throughout the United States, including the New York, New Jersey, and Illinois locations where Plaintiffs' purchases were made.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the Class contains members of diverse citizenship from Defendant, and the amount in controversy exceeds $5 million.

12. This Court has personal jurisdiction over Defendant because Defendant is

authorized to and conducts, substantial business in New York, generally, and this District, specifically. Defendant owns and operates retail locations within this District and throughout New York State.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District as Defendant operates retail locations within this District, Plaintiffs A. O'Brien and J. O'Brien (the "O'Briens") reside here, and their purchases took place at Defendant's retail stores located within this District.

DEFENDANT'S COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION AND PAYMENT CARD DATA

14. Defendant is an American home improvement and construction retail store. Millions of Americans regularly shop at Defendant's online and brick-and-mortar stores. Defendant is the largest home improvement retailer in the United States, and the fourth largest domestic retailer by revenue.

15. When individuals transact business with Defendant, or simply visit one of its stores or website, Defendant collects a wide variety of Personally Identifiable Information (PII) and Payment Card Data ("PCD") about them.

16. Defendant discloses the Information it collects about individuals who either shop online or in stores – or simply enter any of its stores or browse its website, even without making a purchase – on its website:

> **Information We Collect**
>
> **Contact information**
> We may collect the names and user names of our customers and other visitors. Additionally, we may collect your purchase history, billing and shipping addresses, phone numbers, email addresses,

> and other digital contact information. We may also collect information that you provide us about others.
>
> **Payment information**
> When you make a purchase we collect your payment information, including information from your credit or debit card, check, PayPal account or gift card. If you apply for a The Home Depot credit card or a home improvement loan, we might collect information related to your application.
>
> **Returns information**
> When you return a product to our stores or request a refund or exchange, we may collect information from you and ask you to provide your government issued ID. We use the information we collect from you and capture off of your government issued ID to help prevent fraud. To learn more about our Returns Policy, click here.
>
> **Demographic information**
> We may collect information about products or services you like, reviews you submit, or where you shop. We might also collect information like your age or gender.
>
> **Location information**
> If you use our mobile websites or applications, we may collect location data obtained from your mobile device's GPS. If you use our websites, we may collect location data obtained from your IP address. We use this location data to find our nearest store to you, product availability at our stores near you and driving directions to our stores.
>
> **Other information**
> If you use our websites, we may collect information about the browser you are using. We might track the pages you visit, look at what website you came from, or what website you visit when you leave us. We collect this information using the tracking tools described here. To control those tools, please read the Your Privacy Preferences section.

<http://www.homedepot.com/c/Privacy_Security> (hyperlinks omitted) (last visited Sept. 9, 2014).

17. Thus, Defendant stores massive amounts of PII and PCD on its servers and utilizes this information to maximize its profits through predictive marketing and other

marketing techniques.

IMPORTANCE OF DATA SECURITY TO PURCHASING DECISIONS

18. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiffs would not have made purchases at Home Depot, or would not have paid as much for them, had they known that Home Depot does not take all necessary precautions to secure their personal and financial data. Home Depot failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Home Depot.

19. Furthermore, when consumers purchase goods at a national retailer, such as Home Depot, they assume that its data security practices and policies are state of the art and that the retailer will use part of the purchase price that consumers pay for such state of the art practices. Consumers thus enter into an implied contract with Defendant that Defendant will adequately secure and protect their Private Information, and will use part of the purchase price of the goods to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Home Depot failed to provide reasonable security measures, thereby breaching its implied contract with Plaintiffs.

VALUE OF PII TO HACKERS

20. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it is less protected and regulated than payment card data.

21. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three

million customers, they also took registration data from 38 million users." Verizon 2014 PCI Compliance Report, available at <http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 9, 2014). Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

22. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id*.

23. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. Unfortunately, and as will be alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, Defendant's approach at maintaining the privacy of Plaintiffs' and Class Members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

LACK OF SEGREGATION OF CARD HOLDER DATA FROM PII

24. Unlike PII data, payment card data is heavily regulated. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

25. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data." PCI DSS v. 2 at 5 (2010) (hereafter PCI Version 2).

26. One PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code. *Id*. at 7.

27. "Network segmentation of, or isolating (segmenting), the cardholder data

environment from the remainder of an entity's network is not a PCI DSS requirement." *Id*. at 10. However, segregation is recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data." *See* Verizon Report at 54.

28. Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a set price. *See, e.g.*, <http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth> (last visited Sept. 9, 2014).

THE DATA BREACH AFFECTING DEFENDANT

29. News of the data breach was first published by a blogger (Brian Krebs of Krebs on Security) on or about September 3, 2014, before Defendant made any attempt whatsoever to notify affected customers. <http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/> (last visited Sept. 9, 2014) (hereinafter, the "Krebs Report").

30. It now appears that the Home Depot data breach was executed using a variant of the same malware used in the December 2013 Target data breach, and that information for payment cards apparently stolen from Home Depot shoppers are turning "up for sale on Rescator[dot]cc, the same underground cybercrime shop that sold millions of cards stolen in the Target attack." < http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Sept. 9, 2014).

31. Furthermore, it now appears that "the Home Depot breach may involve compromised store transactions going back at least several months." *Id.*

32. The Krebs Report indicates that the cybercrime store rescator.cc (the "Rescator website") listed consumer credit cards for sale that, with the unique ZIP code and other card data,

at least four banks have mapped back to previous transactions at Home Depot. The Krebs Report explained that "experienced crooks prefer to purchase cards that were stolen from stores near them, because they know that using the cards for fraudulent purchases in the same geographic area as the legitimate cardholder is less likely to trigger alerts about suspicious transactions — alerts that could render the stolen card data worthless for the thieves." The Krebs Report indicated a "staggering 99.4 percent overlap" between the unique ZIP codes represented on the Rescator website and those of Home Depot stores, strongly suggesting that the source of the breached credit card data was from Home Depot. *Id.*

33. The ZIP code information the Krebs Report pulled from the Rescator website appears to represent the vast majority, if not all, of Defendant's approximately 2,200 domestic retail locations. The Krebs Report further indicated that, based on conversations with affected banks, this data breach "probably started in late April or early May" and may be ongoing, potentially dwarfing the 40 million debit and credit cards affected by the recent Target data breach (which had 1,800 stores affected during a period of approximately 3 weeks). *Id.*

34. After this news broke, Defendant released an ambiguous and uninformative statement concerning the data breach that failed to confirm the breach, and still did not notify affected customers directly. Rather, Defendant posted the statement on a difficult-to-locate press page on its corporate website (not on the shopping site regularly accessed by customers) sometime after the Krebs Report, vaguely indicating:

> **Message to our customers about news reports of a possible payment data breach.**
>
> We're looking into some unusual activity that might indicate a possible payment data breach and we're working with our banking partners and law enforcement to investigate. We know that this news may be concerning and we apologize for the worry this can create. If we confirm a breach has occurred, we will make sure our

customers are notified immediately. <https://corporate.homedepot.com/mediacenter/pages/statement1.aspx> (last visited Sept. 4, 2014).

35. On September 3, 2014, Defendant could not confirm whether a data breach occurred, but indicated it first learned of a "potential breach" on September 2, 2014, at least one day before the Krebs Report. <http://online.wsj.com/articles/home-depot-tries-to-reassure-customers-about-possible-data-breach-1409743851> (last visited Sept. 9, 2014).

36. On September 8, 2014, Defendant confirmed that its systems "have in fact been breached, which could potentially impact any customer that has used their payment card at our U.S. and Canadian stores, from April forward." <https://corporate.homedepot.com /mediacenter/pages/ statement1.aspx> (last visited Sept. 9, 2014).

37. Defendant has not indicated whether social security numbers, PIN numbers and dates of birth were compromised, nor has it disclosed whether the wide range of other PII that it collects, including names, addresses, telephone numbers, mobile telephone numbers, driver's license numbers, bank account numbers, email addresses, computer IP addresses, and location information, were disclosed in the breach. <http://www.homedepot.com/c/Privacy_Security> (last visited Sept. 9, 2014).

38. Without such detailed disclosure, Plaintiffs and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

39. If fraud were occurring from late April to early September of 2014, because hackers already had their hands on cardholder data and PII, credit card company analytics and other methods (undercover investigations of the black market) would likely have discovered it

before September 2, 2014. Defendant has failed to provide a cogent picture of how the data breach occurred and its full effects on customers' PII and PCD information.

40. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors. On information and belief, while hackers scoured Defendant's networks to find a way to access PCD, they had access to and collected the PII stored on Defendant's networks.

CONSEQUENCES OF DEFENDANT'S CONDUCT

41. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

42. The ramifications of Defendant's failure to keep Class members' data secure are severe.

43. The information Defendant compromised, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC Interactive Toolkit, *Fighting Back Against Identity Theft*, available at <http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf> (last visited Sept. 9, 2014). Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. *Id.* The FTC estimates that as many as 10 million Americans have their identities stolen each year. *Id.*

44. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical

treatment on your health insurance." FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/0271-signs-identity-theft> (last visited Sept. 9, 2014).

45. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud." *See* 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/276> (last visited Sept. 9, 2014) (the "2013 Identity Fraud Report"). Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year. *Id.*

46. Identity thieves can use personal information such as that of Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

47. In addition, identity thieves may get medical services using consumers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

48. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Sept. 9, 2014). In fact, the BJS reported, "resolving the problems caused by

identity theft [could] take more than a year for some victims." *Id*. at 11.

49. Annual monetary losses from identity theft are in the billions of dollars.

50. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013. *See* 2013 Identity Fraud Report.

51. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Sept. 9, 2014).

52. Plaintiffs and the Class they seek to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

PLAINTIFFS AND CLASS MEMBERS SUFFERED DAMAGES

53. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiffs' and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Home Depot's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security

and confidentiality of Plaintiffs' and Class members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

54. Plaintiffs' and Class members' Private Information is private and sensitive in nature and was left inadequately protected by Home Depot. Home Depot did not obtain Plaintiffs' and Class members' consent to disclose their Private Information to any other person as required by applicable law and industry standards.

55. As a direct and proximate result of Home Depot's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

56. Home Depot's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. actual identity fraud or identity theft;

b. the imminent risk of future identify fraud and identity theft;

c. the untimely and inadequate notification of the Data Breach;

d. improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of

their time reasonably incurred to remedy or mitigate the effects of identity theft and identity fraud;

g. ascertainable losses in the form of deprivation of the value of their PII/PCD, for which there is a well-established national and international market;

h. ascertainable losses in the form of economic injury stemming from Home Depot's failure to secure their Private Information, which they paid for as part of price of each product purchased at Home Depot;

i. deprivation of rights they possess under FCRA; and

j. deprivation of rights they possess under the Illinois, New Jersey and New York consumer protection statutes.

57. Damages can also be ascertained and measured by the average black market prices for Plaintiffs' PII/PCD.

58. Notwithstanding Home Depot's wrongful actions and inaction and the resulting Data Breach, Home Depot has offered consumers only one year of credit monitoring and identity theft protection services. This offer is insufficient because, *inter alia*, it does not address many categories of damages being sought. The cost of adequate and appropriate coverage, or insurance, against the loss position Home Depot has placed Plaintiffs and Class members in, is ascertainable and is a determination appropriate for the trier of fact.

59. Home Depot's offer of one-year of free identity protection services, including credit monitoring, is also insufficient because, as the GAO reported, the PII/PCD could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection expires.

CLASS ACTION ALLEGATIONS

60. Plaintiffs seek relief in their individual capacity and seek to represent a class consisting of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of a national class and three subclasses. The national class is initially defined as follows:

> All persons whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014.

61. The three subclasses are initially defined as follows:

> Subclass 1: All persons who reside in the State of New York whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "New York Class").
>
> Subclass 2: All persons who reside in the State of New Jersey whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "New Jersey Class").
>
> Subclass 3: All persons who reside in the State of Illinois whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "Illinois Class").

62. Excluded from the Class and the New York, New Jersey and Illionis Classes are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

63. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is in the millions.

64. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law

and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Class members' personal and/or financial information;

b. Whether Defendant unreasonably delayed in notifying affected customers of the data breach;

c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

d. Whether Defendant's conduct was negligent;

e. Whether Defendant's negligence caused harm to Plaintiffs and the Class;

f. Whether Defendant's conduct violated New York General Business Law Section 349;

g. Whether Defendant's conduct violated the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

h. Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*;

i. Whether Defendant breached its implied contract to Plaintiffs and the Class;

j. Whether Defendant violated the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*; and

k. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

65. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of

other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by Defendant.

66. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

67. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

68. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

69. Defendant has acted or refused to act on grounds that apply generally to the class, as alleged above, and certification is proper under Rule 23(b)(2).

COUNT I

Willful Violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*

(On Behalf of All Plaintiffs and All Other Similarly Situated United States Consumers)

70. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

71. Plaintiffs bring this claim individually and on behalf of a nationwide Class.

72. One of the fundamental purposes of the Fair Credit Reporting Act ("FCRA") is to protect consumers' privacy. 15 U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential. 15 U.S.C. § 1681(b).

73. The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy, and proper utilization of such information. 15 U.S.C. § 1681(b).

74. The FCRA allows for a private right of action against any consumer reporting agency for the negligent or willful violation of any duty imposed under the statute.

75. The FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

76. The FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C § 1681a(d).

77. Defendant is a consumer reporting agency. On a cooperative nonprofit basis or for monetary fees, Defendant regularly assembles consumer credit information, including, among other things, a consumer's credit and debit card account information, names, purchase history, billing and shipping addresses, phone numbers, email addresses, and other digital contact information. Defendant also regularly utilizes interstate commerce to furnish such information on consumers (consumer reports) to third parties.

78. Plaintiffs' and Class Members' PII/PCD constitute Consumer Reports under FCRA, because this information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and the other Class Members' eligibility for credit to be used primarily for personal, family, or household purposes.

79. FCRA requires the adoption of reasonable procedures with regard to, *inter alia*, the confidentiality and proper utilization of personal and insurance information. 15 U.S.C. § 1681(b). FCRA also requires that consumer reporting agencies "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e.

80. Defendant failed to adopt and maintain these and other reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

81. On information and belief, Defendant failed to take reasonable and appropriate measures to secure and protect Plaintiffs' and Class Members' PII/PCD. Defendant also failed to place itself in a position to immediately notify Plaintiffs and Class members about the Data Breach.

82. Home Depot's failure to protect and safeguard the PII/PCD of Plaintiffs and Class members resulted in the disclosure of such information to one or more third parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Home Depot received the PII/PCD, nor was it otherwise permitted by statute, regulation, or order to disseminate such information to unauthorized third parties.

83. Defendant's violations of FCRA, as set forth above, were willful or, at the very least, reckless, constituting willfulness.

84. As a result of Defendant's willful or reckless failure to adopt and maintain reasonable procedures to limit the furnishing of Plaintiffs' and Class Members' PII/PCD to the purposes listed under 15 U.S.C. § 1681b, Plaintiffs' and the other Class Members' PII/PCD was disseminated to unauthorized third parties, compromised, and stolen. Plaintiffs suffered individual harm as a result of Defendant's willful or reckless violations of FCRA.

85. As a further direct or proximate result of Defendant's willful or reckless violations of FCRA, as described above, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in Paragraphs 53 through 59 of this Class Action Complaint.

86. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages (as described in detail in Paragraphs 53-59 of this Class Action Complaint) or statutory damages of not less than $100, and not more than $1,000, each, as well as attorneys' fees, punitive damages, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

COUNT II

Negligent Violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*

(On Behalf of All Plaintiffs and All Other Similarly Situated United States Consumers)

87. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 86 as if fully set forth herein.

88. Plaintiffs bring this claim individually and on behalf of a nationwide Class.

89. Defendant negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

90. Plaintiffs' and the other Class members' PII/PCD was wrongfully disseminated to one or more third-parties in violation of FCRA as a direct and foreseeable result of Defendant's failure to adopt and maintain such reasonable procedures.

91. As a direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs' and Class members' PII/PCD was made accessible to unauthorized third parties in the public domain, compromised, and stolen. Plaintiffs suffered individual harm as a result of Defendant's negligent violations of FCRA.

92. As a further direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in Paragraphs 53

through 59 of this Class Action Complaint.

93. Plaintiffs and the other Class members, therefore, are entitled to compensation for their actual damages (as described in detail in Paragraphs 53-59 of this Class Action Complaint), as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o.

COUNT III

Violation of New York General Business Law § 349

(On Behalf of the O'Briens and All Other Similarly Situated New York Consumers)

94. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

95. The O'Briens bring this claim individually and on behalf of New York Class members. The O'Briens and New York Class members are individuals who reside in New York and whose personal and/or financial information was disclosed in the data incursion on Defendant in 2014.

96. As fully alleged above, Defendant engaged in unfair and deceptive acts and practices in violation of Section 349 of the New York General Business Law.

97. Reasonable consumers would be misled by Defendant's misrepresentations and/or omissions concerning the security of their personal information, because they understand that national retail companies that take credit and/or debit card information and collect PII from customers will properly safeguard that private information in a manner consistent with industry standards and practices.

98. Defendant did not inform customers that it failed to properly safeguard their private information, thus misleading the O'Briens and New York Class members in violation of Section 349. Such misrepresentation was material because the O'Briens and New York Class

members entrusted Defendant with their private information when shopping online or visiting Defendant's stores.

99. Had the O'Briens and New York Class members known of Defendant's failure to maintain adequate security measures to protect their private information, the O'Briens and New York Class members would not have made purchases at Defendant's retail stores, shopped there online or otherwise entrusted their private information to Defendant.

100. As a direct and proximate result of Defendant's violations, the O'Briens and the New York Class suffered injury in fact and loss, including loss of time and money monitoring their finances for future fraud, and the other damages described in detail in Paragraphs 53 through 59 of this Class Action Complaint.

101. The O'Briens seek restitution on behalf of New York Class members.

102. The O'Briens seek injunctive relief on behalf of New York Class members in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

103. The O'Briens seek attorney's fees and damages to the fullest extent permitted under N.Y. G.B.L. § 349(h).

COUNT IV

Violation of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2, *et seq.*

(On Behalf of Plaintiffs Gorman and Ames and All Other Similarly Situated New Jersey Consumers)

104. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1

through 69 as if fully set forth herein.

105. Plaintiffs Gorman and Ames bring this claim individually and on behalf of New Jersey Class members. Plaintiffs Gorman and Ames and New Jersey Class members are individuals who reside in New Jersey and whose personal and/or financial information was disclosed in the data incursion on Defendant in 2014.

106. The New Jersey Consumer Fraud Act ("NJCFA") protects consumers against "any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . ." N.J.S.A. § 56:8-2.

107. In enacting the Identity Theft Prevention Act, which among other things, amended the New Jersey Consumer Fraud Act, the New Jersey Legislature found that "[i]dentity theft is an act that violates the privacy of our citizens and ruins their good names: victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories." N.J.S.A. § 56:11-45.

108. Plaintiffs Gorman and Ames and New Jersey Class members are consumers who made purchases at Defendant's retail stores for personal, family, or household use.

109. Prior to Plaintiffs Gorman and Ames and New Jersey Class members' purchases at Defendant's stores, Defendant violated the NJCFA by affirmatively representing that Plaintiff Gorman and New Jersey Class members' Private Information would be collected and stored securely. Defendant also engaged in unlawful conduct in violation of the NJCFA by making knowing and intentional omissions regarding the inadequacy of its data security systems.

110. Defendant knew or should have known its data security systems and procedures

were inadequate. Defendant did not fully and truthfully disclose to its customers the inadequate nature of its data security systems, omitting material facts that they were under a duty to disclose to Plaintiffs Gorman and Ames and New Jersey Class members.

111. Plaintiffs Gorman and Ames and New Jersey Class members reasonably expected that their Private Information would be securely collected and maintained such that the data breach would not occur.

112. As a result, Plaintiffs Gorman and Ames and New Jersey Class members were fraudulently induced to make purchases and provide their Private Information to Defendant without knowledge of Defendant's inadequate data security systems and procedures. These facts that Defendant concealed were solely within its possession.

113. Defendant intended that Plaintiffs Gorman and Ames and all New Jersey Class members rely on the acts of concealment and omissions, so that they would make purchases at Defendant's retail stores.

114. If Plaintiffs Gorman and Ames and New Jersey Class members knew about Defendant's inadequate data security and procedures, they would not have used their debit and/or credit cards to make purchases at Defendant's stores.

115. Defendant's conduct caused Plaintiffs Gorman and Ames and New Jersey Class members to suffer an ascertainable loss. Plaintiffs Gorman and Ames and New Jersey Class members have suffered an ascertainable loss by having their Private Information compromised, including those damages described in detail in Paragraphs 55 through 59 of this Class Action Complaint.

//

//

COUNT V

Violation of Illinois Consumer Fraud and Deceptive Business Practices Act,

815 ILCS 505/1, *et seq.*

(On Behalf of Plaintiff Griffin and All Other Similarly Situated Illinois Consumers)

116. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

117. Plaintiff Griffin brings this claim individually and on behalf of Illinois Class members. Plaintiff Griffin and Illinois Class members are individuals who reside in Illinois and whose personal and/or financial information was disclosed in the data incursion on Defendant in 2014.

118. Plaintiff Griffin and other Illinois Class members were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their Private Information.

119. Defendant intended for Plaintiff Griffin and other Illinois Class members to rely on Defendant to protect the information furnished to it in connection with debit and credit card transactions and/or otherwise collected by Defendant, in such manner that Plaintiffs' and other Illinois Class members' Private Information would be protected, secure and not susceptible to access from unauthorized third parties.

120. Defendant instead handled Plaintiff Griffin and other Illinois Class members' Private Information in such manner that it was compromised.

121. Defendant failed to follow industry best practices concerning data security or was negligent in preventing the Data Breach from occurring.

122. It was foreseeable that Defendant's willful indifference or negligent course of conduct in handling Private Information it collected would put that information at the risk of compromise by data thieves.

123. On information and belief, Defendant benefited from mishandling the Private Information of customers because, by not taking effective measures to secure this information, Defendant saved on the cost of providing data security.

124. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiff Griffin and Illinois Class Members' reliance on Defendant's deception that their Private Information was secure.

125. Defendant violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff Griffin and other Illinois Class members' Private Information.

126. Defendant's acts or practice of failing to employ reasonable and appropriate security measures to protect Private Information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a), which Illinois courts consider when evaluating claims under 815 ILCS 505/2.

127. Defendant's conduct constitutes unfair acts or practices as defined in that statute because Defendant caused substantial injury to Illinois Class members, which injury is not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

128. Defendant also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the data breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et. seq*., which provides, at Section 10:

Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

129. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

130. Plaintiff Griffin and other Illinois Class members have suffered injury in fact and actual damages including lost money and property as a result of Defendant's violations of 815 ILCS 505/2, including those damages described in detail in Paragraphs 59 through 65 of this Class Action Complaint.

131. Defendant's fraudulent and deceptive behavior proximately caused Plaintiff Griffin and Illinois Class members' injuries, and Defendant conducted itself with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

COUNT VI

Failure to Expediently Notify Following Security Breach in Violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-2 et seq.

(On Behalf of Plaintiffs Gorman and Ames and All Other Similarly Situated New Jersey Consumers)

132. Plaintiffs incorporate the substantive allegations contained Paragraphs 1 through 69 as if fully set forth herein.

133. Plaintiffs Gorman and Ames bring this claim individually and on behalf of New Jersey Class members. Plaintiffs Gorman and Ames and New Jersey Class members are

individuals who reside in New Jersey and whose personal and/or financial information was disclosed in the Data Breach on Defendant in 2014.

134. As stated above, the New Jersey Consumer Fraud Act provides that it is "an unlawful practice and a violation of P.L. 1960 c. 39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate" Sections 56:8-161-164 of that Act.

135. Section 56:8-163 of the New Jersey consumer Fraud Act requires that a business conducting business in New Jersey:

> shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

N.J.S.A. § 56:8-163.

136. The New Jersey Consumer Fraud Act defines a breach of security as follows:

> "Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56:8-161.

137. The 2014 Data Breach at Home Depot constituted a breach of security.

138. Defendant's disclosure regarding the breach of security to Plaintiffs and Class

members was delayed and not made in the most expedient time possible.

139. As a result of the foregoing, Plaintiffs and New Jersey Class members suffered and will continue to suffer ascertainable losses and other damage as described in detail in Paragraphs 53 through 59 of this Class Action Complaint, and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

COUNT VII

Violation of the Illinois Personal Information Act , 815 ILCS 530/1

(On Behalf of Plaintiff Griffin and All Other Similarly Situated Illinois Consumers)

140. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

141. Plaintiff Griffin brings this claim individually and on behalf of Illinois Class members. Plaintiff Griffin and Illinois Class members are individuals who reside in Illinois and whose personal and/or financial information was disclosed in the data incursion on Defendant in 2014.

142. The Illinois Personal Information Protection Act, 815 ILCS 530/1 ("PIPA"), requires data collectors who own personal information concerning an Illinois resident to notify the resident of a data breach "in the most expedient time possible and without unreasonable delay ...." 815 Ill. Comp. Stat. 530/10.

143. Defendant is a data collector within the meaning of the PIPA.

144. Defendant possessed Plaintiffs' and Class members' personal information, as defined by the PIPA.

145. Defendant failed to notify Plaintiff Griffin of the Data Breach in the most expedient time possible and without unreasonable delay.

146. Defendant's failure to timely provide notice constitutes a violation of the PIPA and other relevant statutes.

147. Plaintiff Griffin, individually and on behalf of Illinois Class members, seek all remedies available under the PIPA, including an injunction to require Defendant's compliance with the PIPA.

COUNT VIII

Breach of Implied Contract

(On Behalf of All Plaintiffs and All Other Similarly Situated Consumers)

148. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

149. Plaintiffs bring this claim individually and on behalf of a nationwide Class.

150. Defendant solicited and invited Plaintiffs and Class members to purchase products at Defendant's stores using their credit or debit cards. Plaintiffs and Class members accepted Defendant's offers and used their credit or debit cards to purchase products at Defendant's stores during the period of the Data Breach.

151. When Plaintiffs and Class members provided their PII and PCD to Defendant to make purchases at Defendant's stores, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards, Plaintiffs and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised.

152. Each purchase at a Home Depot store made by Plaintiffs and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract

with Defendant under which Defendant agreed to safeguard and protect Plaintiffs' and Class members' PII and PCD, including all information contained in the magnetic stripe of Plaintiffs' and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

153. Plaintiffs and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards, to Defendant to purchase products at Defendant's stores in the absence of the implied contract between them and Defendant.

154. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

155. Defendant breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect the PII and PCD of Plaintiffs and Class members and by failing to provide timely and accurate notice to them that their PII and PCD was compromised in and as a result of the Data Breach.

156. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail in Paragraphs 53 through 59 of this Class Action Complaint.

COUNT IX

Unjust Enrichment

(On Behalf of All Plaintiffs and All Other Similarly Situated Consumers)

157. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

158. Plaintiffs bring this claim individually and on behalf of a nationwide Class.

159. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monies paid for the purchase of goods from Defendant during the period of the Data Breach.

160. Defendant has knowledge of the benefits conferred directly upon it by Plaintiffs and Class members.

161. A portion of the monies paid for the purchase of goods by Plaintiffs and Class members to Defendant during the period of the Data Breach was supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class members' PII and PCD.

162. Defendant failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiffs and Class members and as a result, Plaintiffs and Class members overpaid Defendant for the goods purchased through use of their credit and debit cards during the period of the Data Breach.

163. Defendant has been unjustly enriched because it has retained the portion of Plaintiffs' and Class members' money that was supposed to have been used by Defendant to cover the administrative costs associated with protecting its members' PII/PCD.

164. It would be inequitable for Defendant to retain the portion of Plaintiffs' and Class Members' money that covered the administrative costs associated with protecting its members' PII/PCD because Defendant misrepresented that it was protecting and safeguarding its customers' PII/PCD when in fact it was not, causing injuries to Plaintiffs and all Class members.

165. Plaintiffs and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in Paragraphs 53 through 59 of this

Class Action Complaint, and seek restitution related to same.

166. Plaintiffs seek restitution or disgorgement of Defendant's ill-gotten gains.

COUNT X

Negligence Under New York Law

(On Behalf of the O'Briens And All Other Similarly Situated New York Consumers)

167. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 69 as if fully set forth herein.

168. The O'Briens bring this claim individually and on behalf of New York Class members. The O'Briens and New York Class members are individuals who reside in New York and whose personal and/or financial information was disclosed in the data incursion on Defendant in 2014.

169. Defendant knowingly collected, came into possession of and maintained Plaintiffs' and New York Class members' Private Information, and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

170. Defendant had and continues to have a duty to timely disclose that Plaintiffs' and New York Class members' Private Information within its possession might have been compromised and precisely the types of information that were compromised.

171. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and New York Class members' Private Information.

172. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and New York Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and New York Class members' Private Information within Defendant's

possession.

173. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and New York Class members' Private Information.

174. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and New York Class members the fact that their Private Information within its possession might have been compromised and precisely the type of PII/PCD compromised.

175. Defendant's negligent and wrongful breach of its duties owed to Plaintiffs and the New York Class proximately caused Plaintiffs' and New York Class members' Private Information to be compromised.

176. As a result of Defendant's ongoing failure to notify Plaintiffs' and New York Class members' regarding what type of PII has been compromised, Plaintiffs and New York Class members are unable to take the necessary precautions to attempt to mitigate their damages by preventing future fraud.

177. Defendant's breach caused Plaintiffs and New York Class members to suffer the loss of time and money monitoring their finances for future fraud.

178. As a result of Defendant's negligent and wrongful breach of its duties, Plaintiffs' and New York Class members' Private Information was compromised and obtained by one or more third parties.

179. Additionally, Plaintiffs and New York Class members are in danger of imminent harm that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

180. Plaintiffs seek an award of actual damages on behalf of New York Class members.

181. Plaintiffs seek injunctive relief on behalf of New York Class members in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII and PCD have been compromised as a result of the Data Breach.

JURY DEMAND

Plaintiffs demand a trial by jury of all claims in this Complaint so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class members' private information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity the type of PII and PCD compromised;

C. For equitable relief requiring restitution and disgorgement of the revenues

wrongfully retained as a result of Defendant's wrongful conduct;

D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

E. For an award of punitive damages;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

Dated: September 10, 2014

Paul C. Whalen, (PW1300)
LAW OFFICES OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, New York 11030
Tel: (516) 627-5610
Fax: (212) 658-9685

Tina Wolfson
Robert Ahdoot
Theodore W. Maya
Bradley K. King
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, California 90069
Tel: (310) 474-9111
Fax: (310) 474-8585

John A. Yanchunis
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
Fax: (813) 223-5402

Counsel for Plaintiffs and the Proposed Class